2021-09

MAINTAINING A COMPETITIVE ADVANTAGE: AN ANALYSIS OF THE EFFICIENCY AND EFFECTIVENESS OF THE MARINE CORPS' ASSESSMENT AND AUTHORIZATION PROCESS

Bucks, Marc B.; Williams, Daphne

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MAINTAINING A COMPETITIVE ADVANTAGE: AN ANALYSIS OF THE EFFICIENCY AND EFFECTIVENESS OF THE MARINE CORPS' ASSESSMENT AND AUTHORIZATION PROCESS

by

Marc B. Bucks and Daphne Williams

September 2021

Thesis Advisor: Joshua A. Kroll
Second Reader: John D. Fulp

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
MAINTAINING A COMPETITIVE ADVANTAGE: AN ANALYSIS OF THE EFFICIENCY AND EFFECTIVENESS OF THE MARINE CORPS' ASSESSMENT AND AUTHORIZATION PROCESS

5. FUNDING NUMBERS

6. AUTHOR(S) Marc B. Bucks and Daphne Williams

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Maintaining a competitive advantage in conflict requires a Marine Corps that can rapidly develop and field technologies to the operational forces. In the 2019 "Commandant's Planning Guidance," the Commandant of the Marine Corps emphasized the need to enhance our capabilities in artificial intelligence, sensor-based data collection, and data-enabled decision-making. Vital to this effort is the Risk Management Framework (RMF), the mandated process by which we assess and mitigate cybersecurity risks to these systems in the rapidly evolving threat environment. To maintain its effectiveness, the Marine Corps must continue to make process improvements that support the rapid development of secure systems. This study conducts a qualitative analysis of the Marine Corps' utilization of the RMF to determine whether current assessment and authorization processes adequately address the current threat environment in a timeline that supports the warfighter. We use a mixed-methods approach to investigate the successes, shortfalls, and inefficiencies of the RMF through the experiences of interviewed subjects involved in the Marine Corps assessment and authorization process. We find that the current Marine Corps assessment and authorization process is slow, stovepiped, and compliance-based. The increasing requirement to develop and field new technologies to the operational forces and the evolving nature of security threats require the Marine Corps to improve its risk mitigation strategy.

14. SUBJECT TERMS RMF, Risk Management Framework, risk management, assessment and authorization, security, ATO	**15. NUMBER OF PAGES** 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MAINTAINING A COMPETITIVE ADVANTAGE: AN ANALYSIS OF THE EFFICIENCY AND EFFECTIVENESS OF THE MARINE CORPS' ASSESSMENT AND AUTHORIZATION PROCESS

Marc B. Bucks
Major, United States Marine Corps
BS, United States Naval Academy, 2009

Daphne Williams
Captain, United States Marine Corps
BS, United States Naval Academy, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Joshua A. Kroll
Advisor

John D. Fulp
Second Reader

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Maintaining a competitive advantage in conflict requires a Marine Corps that can rapidly develop and field technologies to the operational forces. In the 2019 "Commandant's Planning Guidance," the Commandant of the Marine Corps emphasized the need to enhance our capabilities in artificial intelligence, sensor-based data collection, and data-enabled decision-making. Vital to this effort is the Risk Management Framework (RMF), the mandated process by which we assess and mitigate cybersecurity risks to these systems in the rapidly evolving threat environment. To maintain its effectiveness, the Marine Corps must continue to make process improvements that support the rapid development of secure systems. This study conducts a qualitative analysis of the Marine Corps' utilization of the RMF to determine whether current assessment and authorization processes adequately address the current threat environment in a timeline that supports the warfighter. We use a mixed-methods approach to investigate the successes, shortfalls, and inefficiencies of the RMF through the experiences of interviewed subjects involved in the Marine Corps assessment and authorization process. We find that the current Marine Corps assessment and authorization process is slow, stovepiped, and compliance-based. The increasing requirement to develop and field new technologies to the operational forces and the evolving nature of security threats require the Marine Corps to improve its risk mitigation strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
ADP	Automatic Data Processing
AO	Authorizing Official
AP	Authorization Package
ATO	Authorization to Operate
C&A	Certification and Authorization
CBM+	Conditions Based Maintenance Plus
CIO	Chief Information Officer
CL	Confidentiality Level
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CPG	Commandant's Planning Guidance
DCI	Deputy Commandant for Information
DCI&L	Deputy Commandant for Installations and Logistics
DCSA	Defense Counterintelligence and Security Agency
DIACAP	DOD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of the Navy
ECSM	Enterprise Cyber Security Manual
eMASS	Enterprise Management Assurance Support Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act

FSCA	Functional Security Control Accessor
GAO	Government Accountability Office
IA	Information Assurance
IATT	Interim Authorization to Test
IC4	Information, Command, Control, Communications and Computers
INFOSEC	Information Security
IS	Information Systems
ISCP	Information System Contingency Plans
ISCM	Information Security Continuous Monitoring
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
JTF-TI	Joint Task Force Transformation Initiative
MAC	Mission Assurance Category
MARFORCYBER	Marine Forces Cyberspace Command
MCAAP	Marine Corps Assessment and Authorization Process
MCCAST	Marine Corps Compliance and Authorization Support Tool
MCEN	Marine Corps Enterprise Network
MCSC	Marine Corps Systems Command
MCTSSA	Marine Corps Tactical Systems Activity
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security System
NVD	National Vulnerability Database
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OT	Operational Technology
PM	Program Manager

PO	Program Office
PNAS	Proceedings of the National Academy of Sciences
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
POR	Program of Record
RMF	Risk Management Framework
SAR	Security Assessment Report
SECNAV	Secretary of the Navy
SCA	Security Control Accessor
SCAA	Security Control Accessor Analysts
SCRAM	Security Cyber Risk Aggregation and Measurement
SCV	Security Control Validators
SDLC	System Development Life cycle
STIG	Security Technical Implementation Guide
UR	User Representative

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like the thank our friends, classmates, and families for their support throughout our time at the Naval Postgraduate School. We would also like to thank the Marines and members of the Marine Corps cybersecurity work force who participated in our study and assisted in making those connections. We could not have been successful in our efforts without their time and willingness to share their experiences.

Most importantly, we would like to thank our thesis advisor, Dr. Joshua Kroll, and second reader, Professor J.D. Fulp, for their expert advice and guidance through this thesis process. We are truly grateful for the amount of time you devoted to our success both in the classroom and in this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In July 2019, General David Berger, the 38th Commandant of the Marine Corps, issued his Commandant's Planning Guidance (CPG) to the force. Within this transformative document, General Berger lays out his vision for the Marine Corps as we depart from more than 20 years of combat in the Middle East, he reorients the force toward countering the expansion of Chinese influence and military power in the Pacific as well as the advancing cyber capabilities of our competitive adversaries. Of particular interest and in a stark contrast from the status quo, General Berger places particular emphasis on our need to invest in emerging technologies to maintain our competitive advantage in combat. He writes, "we must prioritize research, development, and fielding of emerging and advanced technologies that are applicable within the seaward and landward portions of the littorals. Technologies such as artificial intelligence, robotics, additive manufacturing, quantum computing, and nanotechnology will continue to change the world - we must be positioned to capture the returns on investment" [1]. To realize a competitive advantage from these technologies, the Marine Corps must analyze the current policies and procedures that guide the development and implementation of information systems (IS) and operational technology (OT) to increase the speed and efficiency that emerging technologies are fielded to the warfighter.

Marine Corps IS and OT are subject to threats that can have devastating effects on operations, equipment, and personnel. Additionally, these threats pose a significant risk to the confidentiality, integrity, and availability of information. The Federal Information Security Modernization Act (FISMA) requires that all Department of Defense (DOD) IS go through a formal authorization process prior to operation and after major modifications that affect the security posture of the system [2]. To maintain compliance with federal law and DOD policy, the Marine Corps requires authorization of systems that operate within the Marine Corps Enterprise Network (MCEN) environment and these systems are reviewed annually to confirm the effectiveness of assigned security controls and their implementation. After years of utilizing the Risk Management Framework (RMF) to guide the assessment and implementation of security controls for Marine Corps systems,

experience has shown that the assessment and authorization process can take upwards of 18 months. This requirement has a significant, negative effect on the speed of implementation of information systems and operational technology. Maintaining a competitive advantage through use of emerging technologies requires the Marine Corps to iterate faster on technology development and the fielding of systems to the warfighter, to do so at greater speed than our adversaries, and without compromising our security posture.

This thesis explores the effectiveness and efficiency of the Marine Corps' utilization of the RMF to achieve an authorization to operate (ATO). Our research seeks to answer two main questions: (1) Are the Marine Corps RMF processes and tools adequate to meet the current and future needs of the Marine Corps? (2) What effect do the Marine Corps' assessment and authorization (A&A) policies and processes have on the speed of implementation and security of information systems? Through an analysis of semi-structured interviews with Marine Corps program offices and members of the Marine Corps cybersecurity work force who play a role the A&A process, we explore which aspects provide overall benefit to the Marine Corps' development and implementation of information technologies and those that hinder our ability to obtain or maintain an advantage over our adversaries.

The objective of this research is to conduct an analysis of the Marine Corps' utilization of the RMF to determine whether current A&A processes, training, and staffing are adequate to accurately identify controls and mitigation strategies for Marine Corps IS on the MCEN in a timeline that supports the warfighter. The selected controls and strategies must balance the benefits to mission against risks driven by constantly evolving cybersecurity threats. This research investigates the successes, shortfalls, and inefficiencies of the RMF through the experiences of interview subjects with respect to A&A of IS in the Marine Corps. Specifically, we seek to understand if gaps in knowledge, manpower, and training exist among personnel who are responsible for executing the process. We also seek to understand whether the intended objectives of the Marine Corps A&A process are realized in the actual execution of the process by PMs and the Marine Corps' cybersecurity work force, or whether a disconnect exists between them. Although we intend to analyze broadly the effect of current staffing of Marine Corps cybersecurity work force personnel

on RMF efficiency, this research does not include a business case analysis of Marine Corps manpower management for cybersecurity professionals.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

Understanding the current state of the Marine Corps' assessment and authorization process for IS requires understanding the evolution of DOD programs that led to the RMF. In 1972, DOD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," laid the groundwork for standardizing the minimum-security requirements for automated information systems. In the 1980s, described as the era of trusted computing, the Department of Defense published the Rainbow Series standards for information security. Prominent among these standards was DOD 5200.28-STD "DOD Trusted Computer System Evaluation Criteria" (the "Orange Book") first published in 1983 and updated in 1985 [3]. Over the following decade, the DOD continued to revise its policies as the Department's use of automated IS continued to expand. In December of 1997, the DOD formalized its Certification and Authorization (C&A) process for information systems with the promulgation of Department of Defense Issuance (DoDI) 5200.40, "DOD Information Technology Security Certification and Accreditation Process" (DITSCAP). A representation of the DITSCAP phases is illustrated in Figure 1.

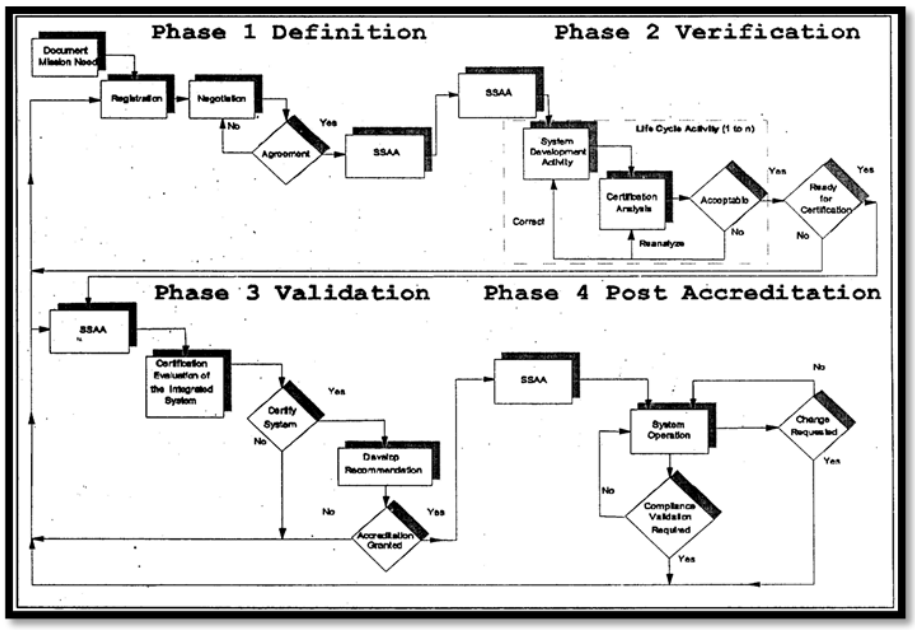

Figure 1. DITSCAP Phases. Source: [4].

As DoDI 5200.40 states, "The objective of the DITSCAP is to establish a DOD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII). The set of activities presented in the DITSCAP standardize the C&A process for single Information Technology (IT) entities that leads to more secure system operations and a more secure DII. The process considers the system mission, environment, and architecture while assessing the impact of operation of that system on the DII" [4]**.** DOD IT "refers to all DOD-owned IT or DOD-controlled IT that receives, processes, stores, displays, or transmits DOD information" [5]. Figure 2 illustrates the many types of systems that fall under the broad definition of DOD IT. DITSCAP served as an important step in the C&A of information systems. DITSCAP was the first standardized process that viewed systems as part of a network infrastructure. Previous processes focused solely on the security of each individual system without the greater context of the environment within which it operated. Furthermore, under the DITSCAP regime, all DOD IT systems require assessment, but only certain categories of systems require authorization before deployment.

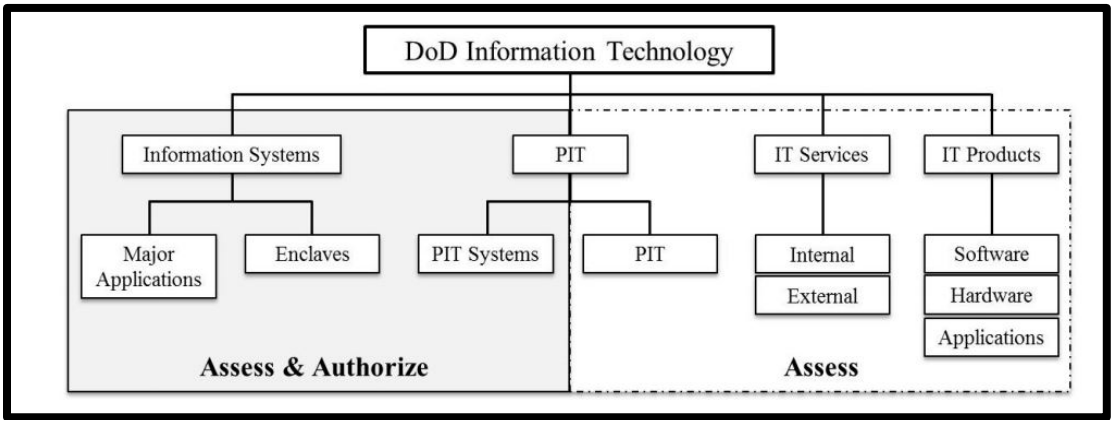

Figure 2. Taxonomy of DOD Information Technology Assessment and Authorization Criteria. Source: [5].

In the post-9/11 era, DITSCAP was unable to address service-specific information security requirements, nor was it able to properly address the Defense Information Systems Agency's (DISA) Ports, Protocols, and Services Management initiatives of the early 2000s.

In addition, DITSCAP lacked a single source for standardized security controls that would facilitate the services and other federal agencies to take a unified approach to security. To maintain cohesion with the NSA's new approach to security, DISA began developing a new framework for securing Federal information systems called the DOD Information Assurance Certification and Accreditation Process (DIACAP).

A. DIACAP

In 2006, DISA developed a replacement for the DITSCAP framework that enabled the DOD to maintain compliance with the Federal Information Security Management Act of 2002, which required all federal agencies to "develop, document, and implement information security programs for systems and information within each agency" [2]. Additionally, FISMA tasked the National Institute of Standards and Technology (NIST) with "responsibilities for standards and guidelines, including the development of standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels; guidelines recommending the types of information and information systems to be included in each category; and minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category" [6]. These standards and guidelines are published as Federal Information Processing Standards (FIPS). FIPS, and other NIST publications, form the standards used by U.S. Government agencies outside the FISMA-designated category of "national security systems" (NSS), which includes DOD ISs and many ISs in the intelligence community and other agencies. FISMA requires standards for NSS to be developed by the Committee on National Security Systems (CNSS), operated by the NSA. For harmony across government agencies, CNSS often adopts NIST standards; we focus on relevant NIST standards as a result, noting explicitly where DOD or CNSS policy requires derogation from widely applicable standards.

The DIACAP framework adopted the use of information assurance controls, developed by the NSA and NIST, to manage information systems across the DOD.

DIACAP followed a multi-step, iterative process to identify and assign information assurance controls based on an analysis of the system. This analysis includes determining the type of information system, the Mission Assurance Category (MAC), Confidentiality Level (CL), required baseline IA Controls, and the controls needed to augment the baseline to meet specific security requirements for the type of information stored, processed, or transmitted.

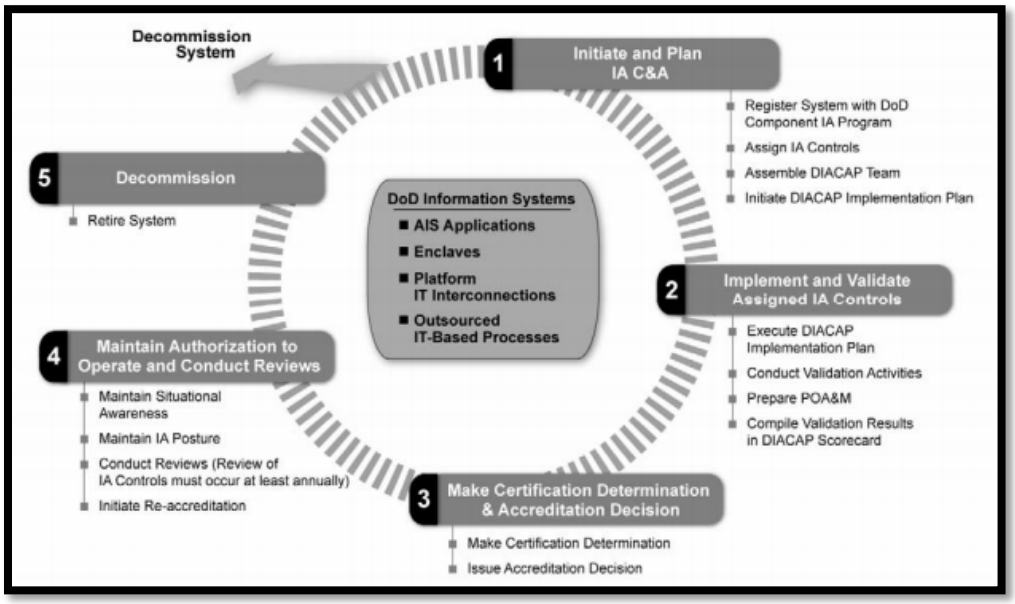

Figure 3. DIACAP Activities. Source: [7].

Although FISMA mandated compliance with FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," and numerous NIST special publications, there was still discretion within the broad-scope guidance that enabled agency-specific solutions to achieve compliance. These variations in implementation had a negative effect on federal agencies' ability to share information across IT systems, and thus reduced the capacity to leverage reciprocity among systems. In response, the intelligence community started an initiative to synchronize its information security processes with the DOD. From this effort, the Joint Task Force Transformation Initiative (JTF-TI) [8] was formed and comprised of members from the DOD, Office of the Director

of National Intelligence (ODNI), NIST, and CNSS. The Task Force began examining the existing NIST publications as the basis to produce a unified information security framework.

Additionally in 2006, NIST codified the baseline security requirements in the release of FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems" [9]. This publication mandated the use of the updated NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," to provide a standard approach to security controls across government organizations. A more comprehensive list of laws and regulations that guide the RMF process are provided in Appendix A.

The revised controls within SP 800-53 detail the most current safeguards and strategies to secure information systems and are reviewed annually by NIST to ensure the most relevant and effective controls are implemented. Figure 4 illustrates the differences between SP 800-53 controls and the legacy controls. To date, there have been four revisions to the original SP 800-53 demonstrating the continuously evolving threat to security and privacy for IS. As federal agencies began implementing standardized controls across systems, the JTF-TI Working Group began establishing a more unified C&A framework to improve security and risk management strategies. The JTF-TI Working Group's efforts resulted in the transformation of DOD IA policies and practices to align with the shifting government risk management policies and practices. In 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" [11], tasking NIST with developing a cybersecurity framework through coordination with federal agencies and leaders of cybersecurity best practices in the private sector. In an extension of the Executive Order, the Office of Management and Budget (OMB) revised Circular No. A-130 [12] in 2016. The Circular promulgates federal policy for information management and codifies the shifting view of security and privacy as compliance requirements to a comprehensive, strategic, and continuous risk-based program.

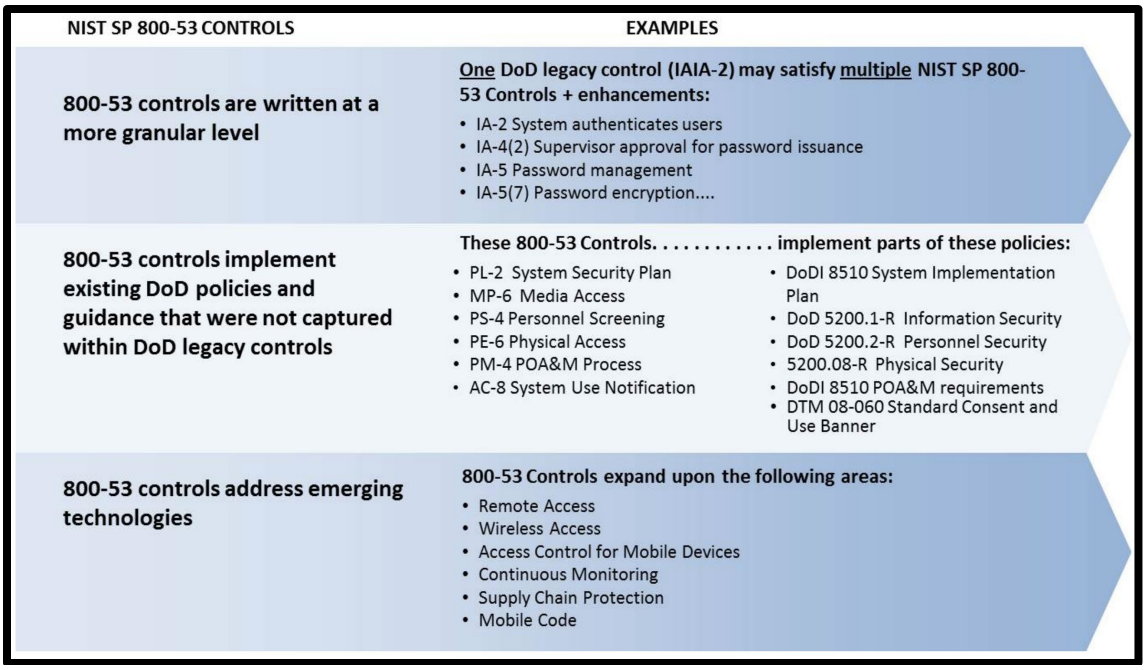

Figure 4. Improvements to NIST SP 800-53 Controls. Source: [10].

B. RMF

NIST, in its partnership with the DOD, ODNI, and CNSS, began transitioning DIACAP to the new cybersecurity framework, referred to in U.S. Government use as the "Risk Management Framework" (RMF) as tasked by the Executive Order. The goal was to "improve information security, strengthen the risk management processes, and encourage reciprocity among federal agencies" [13]. The transition to RMF shifted the focus from compliance checks to new approach that focuses on effective management of risk in diverse environments. Changes from the DIACAP security framework include: replacement of MAC and CL determinations with Impact Value and Security Objective assessments to synchronize language with NIST recommendations and Intelligence Community practices; replacing DOD-defined security controls with updated DOD guidance regarding the assignment, validation and implementation of SP 800-53 controls to align with NIST and the intelligence community; and transitioning the C&A process to an A&A process [8].

The RMF was designed to facilitate the protection of IS by guiding program offices (PO) to identify and incorporate security controls throughout the system development life

cycle (SDLC) [14]. Through continuous monitoring and annual security reviews, program offices can maintain situational awareness of the security posture of systems authorized to operate on DOD networks. The RMF also provides detailed information on the risk associated with the implementation and use of systems to Authorizing Officials to enable authorization to operate decisions [14]. Until a system receives a full or interim authorization, it cannot be connected to the MCEN or any other DOD network In a presentation titled "DIACAP to RMF Transformation Brief" [8], the DOD Cybersecurity Policy Directorate provided a list of benefits to several different stakeholders within the DOD. Although more than ten benefits to the transition were cited, there are two categories that are of particular interest to this research: speed and security. The Cybersecurity Policy Directorate asserts that the RMF will provide more rapid deployment of solutions to the warfighter and will provide greater assurance that systems are secure. Although these were the anticipated benefits prior to the implementation of the RMF, this work assesses whether the RMF has assisted the DOD in realizing these goals, or whether further process refinements are required. Additionally, there is sufficient reason to question whether the RMF has made significant improvements to the security of our systems. It can be argued that RMF has improved standardization of controls across the services and increased the granularity at which the DOD assesses, categorizes, and selects security controls to mitigate risk. However, it may be the case that security risks might be mitigated only by a combination of controls or that controls that appear to fix one risk might cause another to emerge. Further, the nature of what a control is designed to prevent might not be clear when it's evaluated on its own instead of as part of a system. Our study will seek to determine if the RMF has made a direct improvement on the security of our systems or whether such a claim is baseless given the subjective nature of the process and the lack of empirical metrics by which to measure security.

1. RMF Process

The RMF process consists of seven steps that parallel the SDLC used by program offices. The NIST SP 800-37, "Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach," guidance is flexible on what order each step

should be implemented, as long as security risk is managed and all requirements are met [14].

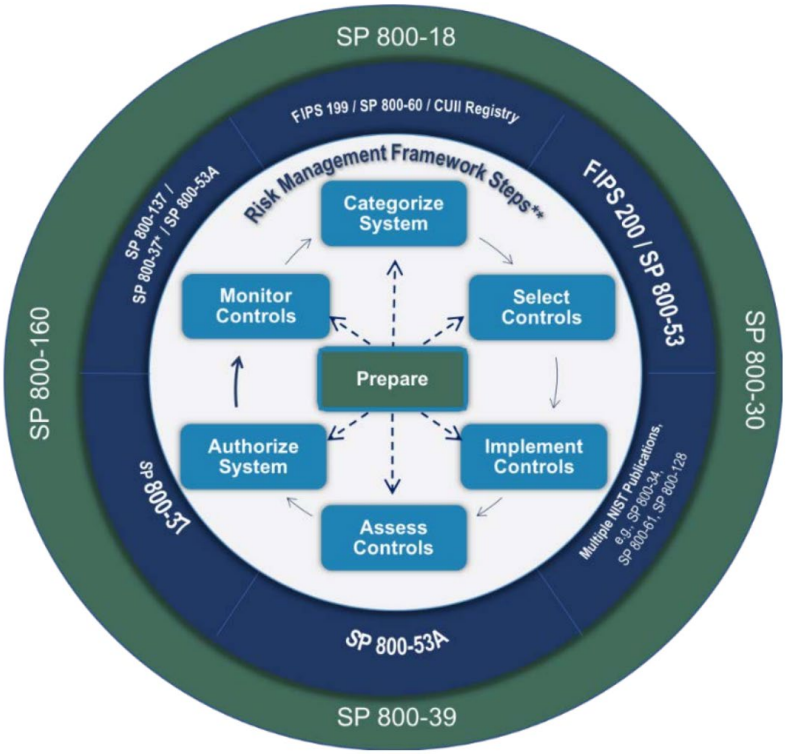

Figure 5. Marine Corps RMF Process. Source: [15].

NIST SP 800-37 Rev.2 (2008) defines the seven RMF steps as follows:

Step 0: Prepare

The first step in the RMF is administrative in nature but establishes an important foundation for the following activities. In this step, system owners take a holistic view of the system to identify stakeholders, system assets, types of information, and information life cycle management. A risk assessment is conducted to identify the vulnerabilities of the system. This is used to prioritize assets based on the severity of impact if information was lost or compromised [14]. Additionally, this step determines where the system should be fit within the overall enterprise architecture and allocates security and privacy requirements used to guide and inform follow on steps of control selection and implementation. System

owners decide how the system will connect to other systems within the established enterprise architecture based off security requirements to guide and inform follow on steps of control selection and implementation.

Step 1: Categorize System

In this step, the system is categorized by impact levels determined from the results of the security analysis conducted in Step 0 with respect to the security objectives of confidentiality, integrity, and availability. In conjunction with NIST special publications, the CNSS Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems" [16], provides amplifying guidance for National Security Systems (NSS) and takes precedence where conflicts arise with SP 800–53.

Figure 6 shows an example of the CNSSI 1253 "Security Control Table" used to categorize systems based on the security objectives, assigning an impact value of low, medium, or high for each of those objectives. In the table, "x"s annotate NIST security controls by impact value and the "+"s annotate additional CNSS security controls by impact value [16]. Controls can be tailored to align to individual systems depending on environmental conditions. The results of this process are included in the security plan and used to develop overlays.

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions			X			X			
AC-2(12)	Account Management | Account Monitoring /	+	+	X	+	+	X			

Figure 6. Example Security Control Table. Source: [16].

Key tasks initiated or completed by the end of this step include categorization of the system in accordance with CNSSI 1253, development of the Initial Security Plan, and updating the security categorization and system characterization information with the requisite DOD component cybersecurity program.

Step 2: Select Security Controls

Once the system is categorized, controls are selected in accordance with the impact value (high, medium, low). The system owner can select a generic baseline of controls that specifically address a certain "group, organization, or community of interest" [14] or customize controls due to requirements. Within SP 800–53, there are more than 900 controls and enhancements that can be selected to apply to IS.

Key tasks for this step include common control identification, selection of security controls, developing an organizational level monitoring plan to verify technical controls are in place, review and approval of the Security Plan, continuous monitoring strategy, and application of security overlays for unique characteristics of the system [14].

Step 3: Implement Security Controls

In Step 3, the security controls identified in the previous step are implemented for the system and organization. Control implementation is documented in a baseline configuration [14].

Key tasks for this step include implementing control solutions and documenting that implementation in the Security Plan.

Step 4: Assess Security Controls

In Step 4, the security controls are evaluated to ensure they are implemented operationally, and the system is working as intended. This assessment is conducted by the Security Control Assessor (SCA). Subsection D.1 provides a description of personnel roles and responsibilities within the Marine Corps' A&A process. Following the assessment, the SCA makes recommendations of approval to the Authorizing Official (AO).

A key deliverable of this step includes development and approval of the Security Assessment Plan, Security Control Assessment, preparation of the Security Assessment Report (SAR) and initial remediation actions [14].

Step 5: Authorize System

In Step 5, the organization's AO makes a final determination on the authorization of an information system. The program office will submit a Security Authorization Package to the AO that will include the Security Plan, SAR, and Plan of Action and Milestones (POA&M)[14]. This package allows the AO to conduct a risk analysis and make an educated decision on whether to authorize the system to operate on the network.

Step 6: Monitor Security Controls

The objective of Step 6 is to determine if the security controls that were selected and implemented on the information system remain necessary and effective. If the environment the system operates within changes, or there are changes to hardware or software that affect the security posture of the system, the system must undergo a reassessment. Updates are reflected in the Security Plan, SAR, and POA&M as needed.

Otherwise, the system will continually be monitored throughout the remainder of the SDLC.

2. Reciprocity

Two of the drivers highlighted in the shift from DIACAP to the RMF were a greater standardization of processes and increased information sharing across Federal agencies, the intelligence community, and the DOD. Reciprocity, as described in Marine Corps' Enterprise Cyber Security Manual (ECSM) 018, is "the mutual agreement among participating enterprises to accept each other's security posture in order to share information" [15]. Leveraging security assessments from like systems not only provides a more rapid understanding of the environment within which the system will operate and a reduction in duplicated work, it can also have meaningful impacts on the speed of implementation of systems. This is especially useful when scaling ISs or OT across networks and platforms. For reciprocity to be leveraged effectively, there must be standardization with respect to assessments, security controls, auditing, and supply chain risk management. The DOD's ability to leverage reciprocity can often be limited by the degree to which categorization, security control implementation, and documentation are conducted uniformly across organizations. The RMF is inherently an interpretive tool and discretion is given to the Services to execute the framework within the bounds of applicable directives, policies, and statutes. Since reciprocity decisions reside at the AO level, the AO has sole discretion as to whether a prior RMF assessment/authorization will be accepted reciprocally. Through our interviews, we seek to understand the degree to which reciprocity was leveraged in any given process, and the amount to which it reduced rework and the timeline for authorization. Conversely, if reciprocity was not sought or was denied, discovery and analysis of these factors may provide useful information for future A&A policy refinements.

C. MARINE CORPS ASSESSMENT AND AUTHORIZATION PROCESS

The latest version of the ECSM 018, "Marine Corps Assessment and Authorization Process (MCAAP)," was published in June of 2020. ECSM 018, is the principal policy and resource document that outlines the techniques and procedures for the authorization of

Marine Corps systems and networks. The MCAAP implements the RMF to maintain compliance with applicable Federal laws and regulations as well as DOD, Department of the Navy (DON), NIST, and Marine Corps directives, instructions, and manuals [15].

The MCAAP provides a standardized A&A structure by which IS and OT are assessed and authorized to preserve the cybersecurity posture of the environment within which the system will operate. The MCAAP utilizes a tiered management structure to identify and mitigate risks to individual systems and the MCEN, as well as monitoring residual risk throughout the program life cycle. In addition to Marines serving as program managers (PM), commanders, and user representatives (UR), the Marine Corps cybersecurity work force plays a prominent role in the development, routing, and approval of authorization packages (AP). The members of this civilian work force serve as subject matter experts within MCAAP for the assessment and mitigation of risks to developmental and existing IS. The delineation of roles and responsibilities within MCAAP is important to understanding the context of the experience of the interview subjects. While some roles are situationally dependent (e.g., PMs, URs), the roles executed by the Marine Corps cybersecurity work force are appointed based on certifications and experience. The MCAAP describes the roles and responsibilities involved in the process, the majority of which were interviewed as part of this study.

1. Roles and Responsibilities

We list the MCAAP roles below. Their assigned responsibilities within the Marine Corps' A&A process are outlined in the ECSM 018:

a. Authorizing Official (AO)

> The AO is a member of the Marine Corps cybersecurity work force and is a senior management official or executive with the authority to formally approve the operation of an IS at an acceptable level of risk. Through authorization, the AO assesses system risk for the IT control environment at the organizational, mission, and business process levels, including consideration of non-USMC systems that may affect financial reporting and operations, and accepts the network and system risks of operating in a specific environment. The Marine Corps has one Service AO, designated as the Marine Corps AO, residing at the Intelligence, Command, Control,

Communications and Computers (IC4) Division in the Office of the Deputy Commandant for Information (DCI).

b. Service Security Control Assessor (Service SCA)

The Service SCA is responsible for ensuring and overseeing a qualified certification cadre (e.g., Security Control Validators (SCVs) also known as Marine Corps Validators, Functional Security Controls Assessors (Functional SCAs), and Security Control Assessor Analysts (SCAAs). The Service SCA provides technical expertise in the preparation and during the conduct of comprehensive security assessments based on the managerial, operational, and technical security requirements documented within the Authorization Package (AP).

c. Functional Security Control Assessor (FSCA)

Functional SCAs are members of the Marine Corps Cybersecurity Work Force and are officials acting under the authority of, and on behalf of, the Service SCA or the AO. FSCAs identify, source, and implement system security requirements on ISs in the acquisition process to provide an acceptable level of risk to the Marine Corps AO. FSCAs also conduct a comprehensive evaluation of the technical and non-technical security features of a system. This includes providing assurance that vendor products used by the ISs have been assessed and authorized, and vendors who develop, store, transmit, or are otherwise involved with Marine Corps systems are subject to the same or higher standards mandated by the Federal Government and DOD.

d. Security Control Validator (SCV)

The SCV is an unbiased trusted agent who provides verification and validation implementation of the system's assigned security controls and safeguards incorporated through the security engineering process. The Marine Corps SCV is responsible for testing the implementation of applicable cybersecurity controls for an assigned system. Validation includes the development of appropriate test procedures, execution of test procedures, and the accurate documentation of a system's security posture based on the validation results and residual risk. Validation is applied throughout the life cycle of an IS to confirm or establish by testing, evaluation, examination, or investigation that an ISs assigned security controls are implemented correctly and effectively.

e. Program Manager (PM)

The PM coordinates all aspects of the system from initial concept, through development, to implementation and system maintenance. The AO, SCA, Information Systems Security Manager (ISSM), SCV, and User

Representative (UR) provide advice, information, and guidance to the PM throughout the authorization process. The PM's function is to ensure that the security requirements are integrated in a way that will result in an acceptable level of risk when operated in its intended environment.

f. Information System Security Manager (ISSM)

The ISSM is the individual responsible to the AO for the Cybersecurity Program of Marine Corps ISs within a particular organization. The ISSM is responsible for the cybersecurity program of a DOD IS and for ensuring compliance to the Marine Corps A&A program. An ISSM will be assigned to support a PM to deliver a Program of Record (POR) with cybersecurity integrated throughout the SLDC or be assigned to a command to perform the day-to-day system security oversight responsibilities, including A&A of operational networks and systems. The ISSM is responsible for the selection of security controls based on the system's security categorization.

g. Information System Security Officer (ISSO)

The ISSO is a member of the Marine Corps Cybersecurity Work Force and is responsible to the ISSM for ensuring that the appropriate operational cybersecurity posture is maintained for a specific DOD IS or organization.

h. Information System Security Engineer (ISSE)

The Information System Security Engineer (ISSE) is a member of the Marine Corps Cybersecurity Work Force and is responsible for ensuring that the ISs information protection requirements are satisfied. ISSE responsibilities include: coordinate with the PM to ensure that all information protection requirements for the IS are identified, ensure the integration of the information protection requirements into IT acquisition processes through purposeful security design or configuration and built in to new IS releases, assist in the development of authorization packages for systems and programs in the developmental and acquisition process, and design the system to meet or exceed the information protection requirements based on security controls during RMF Step 3.

i. User Representative (UR)

The UR represents the operational interests of the user community and ensures the IS meets the user needs. In the Marine Corps this responsibility will include representatives from Marine Forces Cyberspace Command (MARFORCYBER) or Operational Units G-3 or S-3. The UR must review the A&A documentation for compliance with the Mission Needs Statement or Initial Operational Capability Statement and for concurrence with the security features of the system. The UR has the responsibility for ensuring that the appropriate cybersecurity controls have

> been identified, assigned, and validated so that the implementation of the cybersecurity controls meet user community needs. The UR will also identify and document any cybersecurity controls that interfere with or otherwise prohibit effective mission execution [15].

ECSM 018 provides descriptions of the authorization decisions that can be made by the AO. It is important to note that these authorization decisions do not last in perpetuity as described in Step 6 of the RMF. Authorization decisions can be modified at any time during the system life cycle. In most cases, these changes occur during the annual review of the IS authorization or in the event of required changes that affect the security posture of the system.

Through a qualitative study, we seek to understand which aspects of MCCAST and the Marine Corps' RMF process present the most significant challenges for Marines and the Marine Corps cybersecurity work force in achieving and maintaining an ATO.

2. Marine Corps Compliance and Authorization Support Tool

The Marine Corps Compliance and Authorization Support Tool (MCCAST), described as "the only official workflow tool used for the RMF process" [15] by the Marine Corps, is the automated environment within which the cybersecurity work force manages the A&A process. While the Army, Navy and Air Force are currently using the Enterprise Mission Assurance Support Service (eMASS) tool, the Marine Corps is the only service using MCCAST. Additionally, there is no interaction between these two workflow tools. As stated in ECSM 018, "The tool was designed to provide dynamic data exchange, cybersecurity status (metrics) and FISMA reporting, vulnerability assessment management, and A&A status tracking. All Marine Corps A&A packages will be developed, processed, tracked, and monitored through the MCCAST" [15]. This central repository increases transparency in the Marine Corps A&A process, facilitates the flow of information among stakeholders at all levels, and generates the necessary control and compliance reports. Once the authorization package has been completed in MCCAST and reviewed by the SCV and SCA, the package is forwarded to the AO for an authorization decision.

Despite the utility and workflow efficiency that MCCAST provides internal to the Marine Corps, questions regarding the efficiency and effectiveness of the Marine Corps' the workflow tool remain. Specifically, what effect does the utilization of a separate workflow tool have on the Marine Corps' ability to maintain awareness of joint capabilities and leverage reciprocity from across the DOD.

D. RELATED WORK

Throughout the course of this study, we discovered several related works that analyze the current practice of risk assessment and security metrics. Existing research on cybersecurity assessment frameworks and their performance is limited, likely a reflection of the difficult and ambiguous nature of measuring security. The cybersecurity community has been unsuccessful in defining standard metrics for security. Currently, to assess risks to IS and OT, the DOD relies on the cybersecurity work force's experience and judgement along with limited-scope structured threat analysis and standardized compliance checks. The work discussed within this section demonstrates other approaches for measuring security.

1. Measuring Cyber Risk

The DOD is one of many organizations working to develop and maintain secure systems. From global corporations to small businesses, these companies are seeking new and innovative ways both to assess cybersecurity risk and implement security measures to control risks and prevent losses. For example, researchers at the Massachusetts Institute of Technology (MIT) have developed a platform that aggregates non-attributed cybersecurity defense and loss data from its customers using secure multi-party computation. The Security Cyber Risk Aggregation and Measurement (SCRAM) platform enables companies to analyze this anonymous data to understand the cybersecurity threat environment and make informed, targeted investments in their own security. In their study, de Castro et al. analyzed adoption rates of security controls against monetary losses from 49 cybersecurity incidents and the security controls implicated in the loss [17]. Of particular interest, the study found that, "…although the firms in our sample have a high level of security adoption and sophistication, losses often come from defenses that are well

developed, adopted, and understood" [17]. The correlation between losses with well-developed defenses led researchers to conclude that compliance-style checklists for security control implementation are insufficient for determining cybersecurity risk and the true security of the system or firm. The SCRAM platform provides a mechanism for reporting control failures and losses through the aggregation of data in a post-failure environment. In the case of the DOD A&A process, analysis is prospective in order to support authorization decisions. There is generally only limited utilization of cybersecurity data to inform future security reviews. The SCRAM platform (or a similar failure reporting mechanism) could be a useful addition to DOD C&A policies and processes. But to employ such a mechanism, the Marine Corps must first possess the capability to collect, aggregate, and analyze cybersecurity data from across the DOD and develop methods to disseminate this information among our program offices and cybersecurity work force.

2. DON RMF and Risk Analysis

In a 2020, Heier and Morales analyzed literature on evaluating risk and the current state of risk analysis and mitigation within the DON with respect to the assessment and authorization of information systems in their Naval Postgraduate School thesis "Quantifying the Risk Management Framework." This analysis found that, "…DON RMF is highly qualitative and lacks standardized definitions, measurements, metrics, and a risk assessment methodology. The qualitative approach of the current RMF is further complicated by the bias, heuristics, groupthink, inconsistency, overconfidence, and overestimation ensuing from subjective inputs manifested throughout the DON RMF" [18]. Additionally, they provided recommendations that address each step of the RMF aimed at reducing the subjective nature of current risk assessments within the DON and advocate for the DON to develop standardized security metrics. Research performed by Heier and Morales made important contributions by highlighting the difficulty the DON faces in evaluating risk to information systems. While their conclusion that "…quantitative measuring is a must for a successful RMF program" may prove useful in certain aspects (e.g., manpower, resource allocation, cost), it may still suffer from the same subjective evaluation as the current approach in assessing the security of an information system.

3. Government Analysis: Compliance vs. Security

In October 2018, the Government Accountability Office (GAO) conducted a review of DOD efforts to harden the cybersecurity vulnerabilities of its weapon systems. The following year, that review resulted in GAO report 19–128, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," [19]. The report describes three main areas of concern: 1) The DOD has difficulty retaining the cybersecurity expertise needed to analyze cyber threats due to the disparate levels of compensation between the public and private sector; 2) the top secret security classification of many DOD systems prevent information from being shared for collective understanding and mitigation; and 3) an evaluation team has months to complete a system review whereas adversaries are not bound by any such development and contract timelines.

In addition to these findings, the GAO report made two specific observations specifically related to the effectiveness of the RMF. First, the selection and implementation of security controls, by itself, is insufficient in determining whether a system is secure. The GAO report observed that tests demonstrated a significant disconnect between the abstract selection and implementation of security controls and something concrete, like the number and severity of issues identified during red-team exercises, and the security achieved. Further, the variation in strategy and methods for implementing security controls can effect on actual security of the system.

The report cited a system where the role-based access controls that were implemented could be subverted due to unencrypted internal system communication. Although appropriate user authentication controls from SP 800-53 were selected and implemented, the system's design still allowed unprivileged users to gain privileged access by observing and harvesting administrator usernames and passwords from the unencrypted internal communications. That is, controls appropriate to mitigate one identified risk were insufficient because their efficacy relied on assumptions about the system's design (i.e., encrypted internal communication) that weren't true and wasn't foreseen by the RMF risk assessment approach. In this case, unencrypted internal communications may not have presented a risk recognizable by the RMF control selection process but was key to the efficacy of user authentication controls. Second, a false perception of the actual security of

the system may exist within program offices for their respective program because of the compliance-based security control selection process within the RMF. The report states:

> Program Officials cited the security controls they applied as the basis for their belief that their systems were secure. For example, officials from a DOD agency we met with expressed confidence in the cybersecurity of their systems but could not point to test results to support their beliefs. Instead, they identified a list of security controls they had implemented. [19].

The report goes on to note that more senior officials believed security controls are "necessary, but not sufficient" and that penetration testing is a better assessment of system security than compliance tests and documentation. Although this assertion may be valid, there remains a concern presented by Herley in a publication titled, "Unfalsibility of Security Claims" [20]. Herley writes, "There is an inherent asymmetry in computer security: Things can be declared insecure by observation, but not the reverse. There is no observation that allows us to declare an arbitrary system or technique secure" [20].

Although the findings of the GAO report do not provide examples of Marine Corps-specific inefficiencies in the selection and implementation of controls, the report demonstrates a broader viewpoint of personnel responsible for executing the RMF process. In their interviews with GAO, Program Officials made direct associations between the selection and implementation of controls and resulting system security; however, the report finds that this activity is more closely associated with compliance than with security. Since the GAO report did not specify the level of cybersecurity expertise, level of software development expertise, or the branch of service of their interview subjects, the relationship between work force perceptions of security and the cyber vulnerabilities could not be attributed directly to the Marine Corps.

4. Credibility of Security Claims from Compliance

Although the GAO makes a valid observation with respect to penetration test results, it is not entirely dissimilar from compliance testing. Penetration testing may suffer from the same one-sided error problem: if you find a problem in a red team exercise, a security concern has been identified and can be corrected. If a security concern exists but is not found by a red team exercise, this remains unknown and the concern persists,

possibly to be exploited by an adversary. Compliance is the same: if security controls are found to be missing, this can be remediated. However, if a compliance exercise confirms the implementation of controls as required, it does not necessarily follow that the system is secure.

In a journal article published by Proceedings of the National Academy of Sciences (PNAS), Herley describes this very concern stating, "…claims that any measure is necessary for security are empirically unfalsifiable. That is, no possible observation contradicts a claim of the form 'if you don't do X you are not secure.' This means that self-correction operates only in one direction" [20]. Herley argues that we can only assert that a system is secure if our measure for security is the success at implementing controls. He notes that current guidance and practices provided by NIST and Department of Homeland Security's Cyber Emergency Response Readiness Team are "tips" and "best practices." Herley suggests that because this guidance is not supported by empirical evidence and are not falsifiable, they are insufficient to make claims as to the true security of the system.

Similar findings were published in 2020 in a paper titled, "Compliance Cautions: Investigating Security Issues Associated with U.S. Digital-Security Standards." Stevens et al. found that, "…when compliance standards are used literally as checklists — a common occurrence, as confirmed by compliance experts — their technical controls and processes are not always sufficient. Security concerns can exist even with perfect compliance" [21]. In their study, researchers conducted qualitative interviews with security auditors from the IRS, credit card companies, and energy companies to determine the effects compliance-based standards on actual security. Of particular significance, the researchers also concluded that the lack of a defined mechanism for reporting security concerns with compliance standards prevented organizational and industry wide adoption of new risk mitigations [21]. When this issue is viewed in context of the Marine Corps' A&A process, the lack of a defined feedback mechanism between user representatives and ISSMs or ISSEs may have a negative, service-wide impact on awareness and adoption of new security risk mitigations.

5. Secretary of the Navy: Cybersecurity Readiness Review

In acknowledgement of the increasing threat to the DON cyberspace domain and in the wake of several compromises of information; then Secretary of the Navy (SECNAV), Richard V. Spencer, directed a comprehensive review of the department's cybersecurity posture. The Secretary of the Navy's Cybersecurity Readiness Review, directed in the fall of 2018, was published in March of 2019. By contrasting the current state of the Department's cyber policy, organization, authorities, and posture against the best practice of industry, the report made several salient observations with respect to training and retention of the cyber work force that are particularly relevant to our research.

The SECNAV Cybersecurity Review went a step farther than the GAO report in its analysis of current processes for risk and threat analysis within the DON. The report observes that the DON lacks a unified approach to achieve cybersecurity resiliency. One example was the Navy's use of the CYBERSAFE program to develop cyber hygiene standards—whereas the Marine Corps established its standards using the RMF. The most concerning however, is the lack of a process to assess the effectiveness of cybersecurity controls in developmental and deployed systems. The report states, "DON has no uniform or effective cybersecurity metrics to quantify the threat, influence resourcing, or operational planning. There is no overarching means to assess DON's risk to mission, lives, or future planning based on ongoing compromises" [22]. Without metrics to assess the effectiveness of cybersecurity controls and strategies, processes for mitigating risk and adversarial threats are relegated to a compliance-based approach rather than the threat-based approach required of today's dynamic, expanding threat environment.

Through our interview study, we seek to determine if the issues identified by the review team in 2019 continue to exist today, and if so, what factors are preventing changes that will enhance our ability to deliver timely and secure capabilities to the warfighter.

III. METHODOLOGY

This research takes a mixed-methods approach to understanding the utilization of the RMF within Marine Corps A&A. This approach combines a sequence of semi-structured interviews, grounded theory analysis of interview content, and an analytical review of the cybersecurity certification literature. Through the administration of semi-structured interviews and targeted requests for information from individuals involved in the A&A process, we identified areas of common experience that either contributed or detracted from the effectiveness and efficiency of achieving an ATO. We selected interview subjects with responsibilities for system ownership, acquisition, security or privacy management oversight, risk assessment, program implementation, and system monitoring. Using commercial software to transcribe each interview, we applied a grounded theory methodology [23], coding the responses of our subjects across interviews for comparative analysis. Chapter II presents an overview of the cybersecurity certification and assessment landscape, as well as our assessment of the literature evaluating the completeness and efficacy of these tools. Our aim is to identify patterns that will inform specific areas of policy and process refinement of the Marine Corps' A&A process, in addition to areas in which training and education must be reinforced.

A. OVERVIEW OF SEMI-STRUCTURED INTERVIEW PROCESS

The data for this research was collected through a qualitative interview study [24] on individuals who hold roles and responsibilities within the Marines Corps' A&A process. Through these interviews, we were able to understand and analyze the structure and process that we ourselves have not experienced. Through reliance on the experience of others in a variety of roles and with a variety of experiences, we construct a well-rounded view of the problem and undertake an exploratory approach to discovering the successes or areas of needed improvement that may be less evident from quantitative data. The human subjects aspects of this work were determined to be minimal risk by the Institutional Review Board (IRB) of the Naval Postgraduate School as well as the Marine Corps Human Research Protection Program (HRPP) Office and the Marine Corps Survey Office.

The qualitative, semi-structured interview approach enabled us to tailor questions for each respondent with respect to the role(s) in which they served, adapting a structured interview guide to make best use of our time with each subject to elicit their specific knowledge and experiences. This allowed each respondent to provide more detailed answers and allowed us the flexibility to follow up on interesting remarks, asking for more examples, explanations, or discussions. The resulting data are thus also richer and more informative than a survey for our purpose of developing an exploratory understanding of the process and the space of potential interventions and improvements.

We obtained a diversified sample of participants using snowball sampling [24]. Once a participant is identified and interviewed, that participant recommends other individuals that could provide personal experiences on the study topic. We then selected among the recommended individuals to build a sample satisfying our goal to diversify participants across roles, ranks, responsibilities, and points of participation in the A&A process.

The interview guide was structured in six sections, establishing a uniform framework from which to analyze and compare shared experiences of the interviewed participants. The categories within each interview include Subject Background, ATO Experiences, Risk/Threat Assessment, Control Selection/Implementation, RMF Speed and Alternative Processes, and RMF Perceptions. Each interview lasted approximately one hour.

Each interview began with the participant's background information to gain insight on their affiliation with either the DOD or military, job or billet description, and any training they had received prior to utilizing the RMF process. Next, the participants were asked a series of questions related to their involvement and experience regarding the ATO process to include training experiences, risk assessment and control implementation for their specific program, and overall perceptions of the RMF process. Our intent for the interviews was to ask open ended questions that would solicit explanatory responses allowing for the greatest amount of information to be garnered in a one-hour interview. Although interviews were limited in time, multiple interview participants agreed to conduct follow-on interviews. As we gained insights from the experiences of interview participants,

we progressively narrowed the scope of follow-on interviews to illuminate specific areas for clarification and expansion.

B. RESEARCH QUESTION

The following questions serve as the foundation from which this study was developed. These questions were not used as the interview guide but instead provided the context by which the interview guide was developed.

1. Do RMF processes and controls adequately address the current threat environment?

2. Is the selection of controls determined based on achieving compliance with Marine Corps requirements or on mitigating concrete risks identified by threat analysis?

3. To what extent do RMF assessments aid or hinder the Program Manager, Security Control Validator, and Authorization Officer in certifying or accrediting the system? Why and how?

4. Is the RMF equally capable of addressing threats to different types of DOD cyber systems?

5. Is the training for program offices and Marine Corps cybersecurity work force members adequate to properly execute and oversee the Marine Corps RMF process?

6. Are security concerns and attendant controls common across some or many Marine Corps information systems?

7. Is the RMF being conducted by program offices and the cybersecurity work force or are contractors being used to conduct the process? If so, why?

8. What effect does the RMF process have on speed of implementation of information systems? Do alternative ATO processes provide a different timeline for implementation?

9. What changes would better facilitate a faster authorization process, while still maintaining or even improving the resultant security posture?

C. DATA COLLECTION

For this research, we conducted qualitative, semi-structured interviews with 25 individuals: both active-duty Marines and civilians. Our subjects were all members of the cybersecurity work force from various organizations within the Marine Corps. Participants had a wide range of experience, ranging from a subject with two years of experience in the Marine Corps only to a subject with more than 30 years of experience spanning three services and each of the information system assessment frameworks from DITSCAP to the current RMF. Our interview subjects include current and past PMs, ISSMs, ISSOs, ISSEs, SCVs, SCAs, and AOs, as well as current Marine Corps Data Systems Specialists who are serving in billets involved with the A&A process or penetration testing activities.

Due to coronavirus-related restrictions, all interviews were conducted by telephone or video conferencing. The interviews were recorded, transcribed using the Dragon Professional speech recognition software, and analyzed under a grounded theory approach utilizing qualitative research software, ATLAS.ti. These software tools supported our ability to code and analyze the interview transcripts to extract common themes.

Prior to the start of interviews, we obtained written and verbal consent from the participants and informed them of our intent to record the discussions for transcription purposes. Participants were encouraged to discuss their experiences with the RMF framework on past and present programs, highlighting both successes and points of friction. The interview guide, provided in Appendix B, was structured to illicit follow-on discussions related to our specific research questions. Our study does not identify interview subjects by name and quotations will not be attributed to the speaker.

IV. FINDINGS

This chapter summarizes the reoccurring themes discovered through the conduct of semi-structured interviews described in Chapter III. The four themes identified include compliance, barriers to reciprocity, the MCCAST functionality, and personnel and training.

A. COMPLIANCE

RMF was designed as a dynamic process to better enable program offices to incorporate cybersecurity into their systems. To facilitate this work, ISSMs, ISSOs, and ISSEs are assigned to programs who then follow the guidelines and best practices developed by NIST and other agencies to mitigate security risks to IS and OT.

We find that in an ideal scenario, IS security teams are in communication with program offices and the user representatives early in the design and development phase of the system to ensure that security requirements are incorporated from the beginning. Starting at Step 0 of the RMF process, security teams work with the user representatives and program offices to gain an understanding of the system, including: an understanding of the environment within which it will operate, the types of information it will store and process, and the placement of the system within the enterprise architecture. When complete, security teams move to Step 1 of the RMF process utilizing the CNSSI 1253, and NIST special publications to categorize the system to determine the impact value of each security objective with respect to the confidentiality, integrity, and availability of the system. The most important part of this process is the data and information that security teams use to make these categorizations. Subjects with less experience or in roles lower in the A&A hierarchy expressed a high level of confidence that categorizations identified at this stage adequately characterized security risks and that controls selected later to mitigate these risks would provide system-level security; by contrast, subjects with more experience or responsibility (i.e., those higher in the A&A hierarchy) expressed greater doubts about this relationship. One interview subject with many years of experience addressed this notion by stating, “Anyone that tells you that if you just do RMF, implement security controls, and the system will be secure will be way off the mark.”

Throughout the course of our interviews, we found that system categorization decisions rely heavily on CNSS instructions, the NIST publications, the National Vulnerability Database (NVD), and the experience of the security team. The Marine Corps does not currently maintain its own repository of security concerns, or control implementations that are known to cause issues, or results of penetration testing of other systems. Therefore, this information does not exist for dissemination to security teams across the Marine Corps and cannot be incorporated into the development of current and future systems.

Reliance on testing against NVD incidents and best-practice publications forces current practices into a compliance-based approach. While some systems undergo penetration testing by the Marine Corps Tactical Systems Support Activity (MCTSSA) Cyber Assessment Team or a Marine Corps Red Team, most systems do not receive this level of scrutiny. Indeed, one subject noted that "unless it is otherwise directed, we are really looking at performance and requirement-based testing." Additionally, particularly with respect to the testing done by MCTSSA, an interview subject stated that the results of penetration testing are not promulgated to program offices, ISSMs, or SCVs for awareness or consideration. This information is only provided to the respective program office so that the vendor may make the necessary corrections or changes to the system, as required. The interview subject implied that this information is not made more widely available to protect the vendor from negative evaluations as a result of poor performance against security testing.

We find a parallel aspect to this concern during the annual security reviews of Marine Corps systems. In addition to the lack of data from other systems, there is currently no feedback mechanism from users or user representatives directly to the ISSEs and ISSMs responsible for ensuring proper mitigation of risk for the respective system. If the program office lacks awareness of security concerns or fails to communicate this information to an ISSE or ISSM, it cannot be considered for security control modifications during the annual review. Several subjects indicated that the same user representative is often used for multiple systems within an organization which affects the level of detail and understanding the individual has regarding each system. As one interview subject puts it:

> Often the challenge is finding who best fills the user representative role. According to the RMF process they are the ones that can most inform what types of data are present in the system and or processed by the system and that forms the basis for the rest of categorization and control selection… It is a challenge to find someone who can say this is what the system will really be doing.

Currently there are no direct lines of communication between security teams and the system users. Security teams often conduct these reviews in the absence of user feedback. The resulting process becomes no more than a confirmation of the original categorization and control implementation. A current ISSM emphasizes:

> You pick a third of your controls based on your information system's continuous monitoring strategy. That is subjective that we have determined how often these things should be analyzed. We run through a tabletop exercise to see if the plan is still applicable as is. We run some scans. Do your STIGs [Security Technical Implementation Guide] to make sure your stuff is running the same level if not better than the year before.

Another interview subject noted the same activities but went on to acknowledge the reality of the effect of the annual review saying. The subject states:

> With the annual security reviews. We only do this once a year and they only review maybe 40 to 50 percent of the controls. That's just the check to make sure that you do what you said you were going to do. That is the only point.

As discussed by Herley [20], confirmation that the security control has been implemented does not mean the system is secure. The way in which security controls are implemented has a direct impact on the security of the system. Failure to implement a single control in a group of controls designed to satisfy a particular security objective can present a vulnerability. Further, only a portion of the total security controls are reviewed and tested at a time. If the security team is responsible for upwards of 10 programs at any given time, there will be multiple programs in the review process, simultaneously. Without the time or resources needed to conduct thorough security review of each system, the Marine Corps currently relies on the required scans and the conduct of a tabletop exercise to meet the requirement.

If the Marine Corps is to improve its security control selection and implementation processes, we must collect and disseminate the findings of their penetration testing events.

This capability will also reduce the amount of rework and changes required of system security configurations to correct the same vulnerabilities. If we expand this concept across the DOD, we can not only increase the security posture of DOD systems but also reduce the time and labor-intensive processes required of the DOD cybersecurity work force.

B. RECIPROCITY: BARRIERS TO UTILIZATION

Two of the motivations for the transition from DIACAP to RMF were an increase in standardization of security controls and better information sharing across Federal agencies, the DOD, and the intelligence community. JTF-TI and NIST were largely successful in providing a unified framework for agencies and departments to approach cybersecurity risk assessment and mitigation. However, we find that the flexibility afforded in implementing this framework enables stovepiped processes under which assessments made by different services, agencies, and even programs are incomparable. This runs contrary to the goal underlying the development of the RMF and limits the Marine Corps' ability to fully leverage reciprocity from like systems across the DOD. Subjects reported difficulty establishing security assessments through reciprocity. We identified three themes in the experiences these subjects conveyed. First, the interpretive nature of selecting and documenting security controls leads AOs to deny requests for reciprocity despite an existing, approved ATO in another service branch. The RMF attributes (e.g., subjective, interpretive) that enable the services to tailor the process in way that best supports their unique requirements are the same attributes create a barrier to the approval of reciprocity. Variations in the implementation and documentation of controls across services were frequently cited as the reason for reciprocity being denied. When asked about the degree to which the Marine Corps leverages reciprocity from other services, one interview subject acknowledged that:

> We really have had no problems accepting reciprocity from other services. Now the other way around, that's a different story. We have had some issues where other services don't want to accept our requests for reciprocity because of the way we do things a bit different.

Another subject expanded on this concern and provided additional insights into the disparities in documentation that negatively affect the acceptance of inter-service reciprocity:

> Reciprocity you would think would be easy. The services don't require the same documents. We have different processes between them. We should be able to grab and use it from one thing to the next. Everything we do is different between the branches. You have to get an interpretation of what they said or what you are looking for.

Second, inefficiency in routing a request for reciprocity extends timelines for achieving an ATO and injects uncertainty into the process. Interview subjects described an "all or nothing" approach to reciprocity that prevents the work force from utilizing the necessary aspects of approved ATO package to support approval of their own. One ISSM recommended routing partial or full requests for reciprocity earlier in the process to prevent timeline delays and the rework that a denial of reciprocity creates by stating, "we should be able to do a delta package that says, 'Here are the differences [between the two packages]...are you willing to accept this.'"

The AO is the final authority on reciprocity decisions. In the current process, ISSMs include documentation for requested reciprocity from other systems within the authorization package. If an ISSM includes a request for reciprocity in an authorization package, they will not receive a decision on the request until the package is reviewed and adjudicated by the AO. In the best case, the request for reciprocity is approved and the amount of time required to complete the assessment, selection of controls, and documentation is reduced. However, we found that this efficient result is not always guaranteed.

Even when reciprocity is granted, there are still limited situations where ISSMs and their teams must still input each of the controls and documentation into MCCAST. Of note, in the cases where this requirement was made, reciprocity was approved from a system outside of the Marine Corps. Since the other services use eMASS and the Marine Corps uses MCCAST, despite the approval, the team still needed transcribe the documentation from eMASS to MCCAST. One interview subject described this scenario stating:

> They have come back and said we need to put all controls in MCCAST. I was granted reciprocity but now I'm still taking all the info that's already in eMASS and I'm putting it into MCCAST, one by one. And this includes all the mitigating [controls] and comments and that is a lot of work.

Although this issue was identified only a few times in interviews, the relatively small size of our interview sample leads us to believe that this example of additional, MCCAST-specific work might contribute to a significant expenditure of resources across the Marine Corps. This issue is further complicated by the fact that the information transcribed into MCCAST is static. If the other service updates their authorization package, and the Marine Corps is not notified, the plan of action and milestones (POA&M) and other documentation becomes stale and there is currently no way to synchronize this information across systems.

In the worst case, if the request is denied, the ISSM and their team must begin the RMF process over again: selecting, implementing, and documenting these same controls. In this case, the inability to leverage reciprocity results in significant delays due to the amount of new compliance work that must be completed despite the existence of an approved ATO elsewhere in DOD. This delay adds on to the months it can take for a package to progress through each approval step in the routing chain including the SCA, SCV, and AO. Additionally, while the package is being routed, the ISSM and their team cannot progress to the next steps of the RMF. Their progress is stopped, and in most cases the team will move on to another one of their other assigned projects. This uncertainty for ISSMs as to whether a reciprocity request will be granted provides a disincentive to leverage reciprocity. If ISSMs are unsure if reciprocity will be approved early in the process, and a denial would cause them to conduct all the analysis and documentation again, they are incentivized to produce authorization packets which are fully under their control, to minimize uncertainty at the cost of increasing workloads and delays prior to ATO approval.

Finally, to leverage reciprocity in an authorization package, a reviewer must first be aware of like systems and understand the environment within which they operate, in order to understand if the previously granted ATO should apply in the scenario under review. Currently, there is no standard mechanism in place by which Marine Corps

cybersecurity teams can review ATO documentation for like systems across the DOD. The Marine Corps cybersecurity work force must either leverage contacts from the program office, rely on personal contacts within other services to seek information about these programs, or request access to eMASS to view the desired ATO package. Facilitating the cybersecurity work force in expanding their awareness of existing programs across the other services will serve to better enable Marine Corps integration with naval and joint force systems and operations. Furthermore, increased awareness of like programs, their respective operational environment, and dependencies will lead to reduced costs, timelines, and rework in the development and implementation of IS and OT.

C. MCCAST: A STOVEPIPED WORKFLOW TOOL

Proper execution of the RMF is a time and labor-intensive process that requires significant communication and teamwork between program offices, user representatives, and the cybersecurity work force. MCCAST is the Marine Corps' sole workflow tool for the execution of the RMF within the A&A process. While MCCAST possesses many positive attributes including a digital repository for information including hardware and software data, system boundary tracking, diagrams, and POA&Ms; we find that it has numerous areas of needed improvement, limits efficient information sharing across the joint force, and is inconsistent with the CPG's emphasis on naval integration.

Currently, the MCCAST workflow tool does not support the communication and interaction with eMASS that is necessary to leverage reciprocity efficiently. In one ISSM's opinion, "when you get to the actual interconnection between systems, it falls well short by not allowing me to specify who I need to inherit from or who I need to connect to." Multiple ISSMs made recommendations for MCCAST functionality that would benefit to their efforts to leverage reciprocity. Several subjects who worked as ISSMs indicated that their efforts to leverage reciprocity would be greatly aided by adding a request function to MCCAST. The described function would enable information security teams to communicate directly with the respective program office from which the reciprocity is being requested. With the significant amount of time and effort it takes to complete an authorization package, we must take advantage of every opportunity to make their

processes more efficient. By reducing barriers to leveraging reciprocity and inheritance, we can reduce the amount time spent categorizing the system, selecting, and implementing controls, and satisfying documentation required to be completed by the cybersecurity work force.

Similarly, participants expressed a need for a parent-child configuration within MCCAST to allow similar programs sharing a common set of controls with the same requirements to fall under one common ATO. A current ISSM gave one such example:

> If you have a system and you get an ATO for it and you want to deploy that somewhere, it is all or nothing. You've got five VMs in there, that site needs to take and deploy all five. You can't take one VM and put it into your system unless you do your own accreditation.

With the push for units to deploy in small, specialized teams, there is no need to take unnecessary equipment and waste resources. This includes the processing power required to operate these emerging technologies. To facilitate this, program offices are trying to break apart and split up resources into smaller packages to better fit the size of deployed units. Without the parent-child relationship, participants reported conducting duplicative work on multiple packages all contributing to a delay in the ATO process. Establishing a policy for program offices to build and deploy packages under one ATO would greatly benefit both the program office and warfighter.

While MCCAST does allow security teams to view other systems within the Marine Corps, the inability to view Navy ATOs demonstrates a disconnect with the Commandants' emphasis on naval integration. Of note, there is an existing memorandum for reciprocity with the Navy. We view this memorandum as the short-term solution for the issues we've identified, and as such, the memorandum does not improve awareness of like systems and packages. We believe clear benefits remain in utilizing a common workflow tool. In addition to the Navy, the Army, the Air Force, DISA, and the Defense Counterintelligence and Security Agency (DCSA) also use eMASS, demonstrating how widely the lack of outside data in MCCAST limits the use of reciprocity and inheritance in Marine Corps ATO adjudication. Interview subjects were unable to provide a reason as to why the Marine Corps uses a separate tool to manage authorization packages. Interview subjects with previous experience using eMASS acknowledged that the tool has issues of its own, but

still believed the benefits of sharing a common tool outweigh those concerns. Further, eMASS is a well-established tool, sponsored by DISA and DOD Chief Information Officer (CIO), with the necessary support for sustainment including upgrades to its functionality in response to evolving requirements and new needs of the cybersecurity work force across the DOD. We find that despite any issues eMASS may have, the ability for ISSMs to share a common workflow tool with the rest of the joint force would promote information sharing (one of the original goals of developing the RMF) and provide greater awareness and efficiency in leveraging reciprocity and inheritance between existing ATOs and newly sought ATOs (another goal that motivated the development of the RMF).

While increased functionality may provide significant benefit to the cybersecurity work force, IC4 does not currently possess the funding or capability to implement updates and changes to MCCAST, no matter how much such changes would improve current processes. Interview subjects explained that MCCAST is not a POR, and as such, does not have allocated funding for improvements or maintenance. ISSMs described the inability to make improvements for attaining an approval for reciprocity as a significant barrier to efficiency. Failure to ensure proper funding for sustainment of MCCAST—including capability to implement changes in response to evolving requirements—increases friction within the Marine Corps' A&A process and thus injects unnecessary friction into the Marine Corps' ability to rapidly develop and field technologies to the warfighter.

D. PERSONNEL AND TRAINING: DOING MORE WITH LESS

The increased need for advanced capabilities and technologies places significant responsibility on program offices and vendors to assess risk for their specific program. These individuals are not always cybersecurity professionals and often rely on DOD instructions, NIST publications, and user representatives to identify risks. At present time, the minimum requirements for Marines to become PMs is a Defense Acquisitions University (DAU) RMF certification (along with other training modules). While the training may be adequate to gain a high-level understanding of the RMF, cybersecurity knowledge has a smaller emphasis within this training. A PM discussing the challenges to gain an understanding of the Marine Corps A&A process admitted that,

> They [Defense Acquisitions University] have a system online like MarineNet. Cybersecurity is mentioned in there but that is the extent of actual learning. You don't retain much. It took me probably a year before I was really able to speak RMF and I don't think I still can do a good job at it. I got to a point where I could finally understand what the ISSM was talking about.

Many of the participants interviewed had to rely heavily on their ISSMs, vendors, and on-the-job training to gain a deeper understanding of cybersecurity risks and requirements. An active-duty Marine described his relationship with his program vendor in executing the RMF, conceded that he has to "truly rely on my vendor and ensure that the vendor knows what they are doing."

In several interviews, members of the cybersecurity work force indicated that Marine Corps does not possess the number of trained cybersecurity professionals required to meet its mission effectively. One interview subject observed:

> We don't have enough people in program offices and acquisition offices to do all the stuff the stuff we are trying to get done […] We push ourselves into investing into a capability and ultimately after three or four years, it gets traction.

This very situation was described with respect to the Conditions Based Maintenance Plus (CBM+) program. Despite the program having a detailed white paper and there being a direct reference to predictive maintenance within the CPG, due to lag in the Program Objective Memorandum (POM) cycle, the CBM+ program is not a POR. Because of this, the program is not being led by a program office and does not have a dedicated information system security team assigned. The responsibility for completion of the original Interim Authorization to Test (IATT) and the current efforts to attain a full ATO relies on the Deputy Commandant for Installations and Logistics' (DC I&L) program lead and the respective vendor to complete the process. Although an ISSM from Marine Corps Systems Command (MCSC) is assigned to provide support to their efforts, this arrangement does not allow for support on a daily basis. The lack of timely process support has resulted in substantial timeline delays to a capability referenced in the CPG , directed by a white letter, and is a current focus of effort of the DC I&L. We find that although this type of situation is more common outside of MCSC, the pace at which such systems are

being developed is overtaking the Marine Corps' ability to put cybersecurity professionals against these requirements. Additionally, the current acquisitions framework and POM cycle does not support the rapid development and fielding of ISs and OT to the warfighter. These issues lead to information system security teams being assigned more programs than they have the time and resources to properly support. A current ISSM noted, "When I was with the Navy, I only had two to three programs at a time. Right now with the Marine Corps, I have double that number or more." Although this research does not include a manpower analysis of the cybersecurity work force, this is an important consideration for future investment by the Marine Corps.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE WORK

This thesis explored the effectiveness and efficiency of the Marine Corps' utilization of the RMF to achieve an authorization to operate (ATO) by focusing on two main questions: (1) Are the Marine Corps RMF processes and tools adequate to meet the current and future needs of the Marine Corps? (2) What effect do the Marine Corps' assessment and authorization (A&A) policies and processes have on the speed of implementation and security of information systems? To answer these questions, we analyzed several related studies on risk assessments and cybersecurity metrics and performed a human subjects study on participants in the Marine Corps' A&A process, conducting 25 semi-structured interviews with Marine Corps cybersecurity personnel responsible for the execution of the RMF and A&A process. The chapter contains a summary of our findings and areas for future research.

A. SUMMARY OF RESEARCH AND FINDINGS

We find that the Marine Corps must improve its current compliance-oriented processes for assessing and mitigating cybersecurity risk, particularly in light of the evolving nature of security threats from adversaries. Evolving cybersecurity threats are poorly countered by a compliance-oriented process. Physical-world security threats and changing adversary behavior both drive new demands and evolving requirements to develop and field new technologies to the operational forces. Our findings suggest that the current RMF process hinders the Marine Corps' ability to respond to both kinds of threat.

Security assessments are conducted by program offices before systems are employed in practice with limited utilization of cybersecurity data to inform future security reviews. We find that these assessments require a substantial degree of interpretation by security assessment team, but also are heavily driven by a rigid compliance mentality and the need to satisfy long checklists of required security controls. Pre-employment testing and annual security reviews are generally focused on verifying implemented controls rather than performing careful analysis of the system's security. As a result, we find that RMF-driven security evaluation results do not correspond to the ability to make claims about a

system's ability to resist compromise by an adversary. This is partly due to the natural one-sided error of security evaluation [25]. It is also due to the fact that the RMF, as put into practice, focuses the attention of evaluators on functional testing of implemented controls rather than attempts to match real system risks (even those which are clear to the evaluators) to mitigating controls.

Further, the Marine Corps has imposed unnecessary barriers to leveraging reciprocity, a regime under which security authorization and an ATO can be achieved by recognizing the evaluation of a system in a different context (for example, the same system deployed by a different service branch). The lack of common security control implementations and documentation standards across the services combined with the fact that the Marine Corps uses its own separate RMF workflow tool, that does not share data about ATOs or evaluations elsewhere in DOD, creates significant inefficiencies and precludes the benefits that reciprocity would provide. Using a Marine Corps-specific tool for the A&A of all emerging technologies for use on the MCEN and DOD networks should not be a contributor to inefficiencies in our processes. Funding and development support for MCCAST is vital to improving the speed and efficiency of delivering capabilities to the warfighter and the Marine Corps ability to iterate faster than our adversaries.

The Marine Corps prides itself on doing things differently than the other services. While it may prove effective in other disciplines, this mindset has led the Marine Corps to create stovepiped processes and tools that prevent a unified cybersecurity effort across the DOD. This creates operational cybersecurity risk for the Marine Corps by limiting its ability to field emerging technologies rapidly and limiting the effectiveness of its cybersecurity assessment processes. If the Marine Corps is to maintain a competitive advantage over our adversaries, we must streamline our processes, leverage reciprocity to the greatest extent possible, and integrate the cybersecurity efforts of the joint force.

B. AREAS FOR FUTURE STUDY

Our research has uncovered several areas of study for future researchers to consider that would provide a direct benefit to the cybersecurity posture of the Marine Corps.

(1) Limitations of Compliance-based Testing

The lack of awareness among the Marine Corps cybersecurity work force of vulnerabilities discovered by users and the limited capability to conduct penetration testing of Marine Corps systems has highlighted the degree to which control selection is driven by system categorization. Without the ability to conduct continuous monitoring, the Marine Corps requires a more robust and thorough approach to security. Future research can explore the degree to which the current compliance-based testing reflects the actual security of Marine Corps systems.

(2) Proof of Concept for Improved MCCAST Functionality

If the Marine Corps is determined to maintain a separate RMF workflow tool, efforts must be made to improve workflow and joint force integration to better support efficiency of interservice and Marine Corps internal reciprocity. Improved functionality would maximize the use of reciprocity and inheritance across the joint force and reduce the amount of duplicative work currently required of the DOD cybersecurity work force. Future work in creation of a proof-of-concept module for MCCAST that allows program managers the ability to link interoperable programs together and enable communication within the workflow tool would be a significant benefit to programs seeking reciprocity.

(3) Quantitative Analysis of the Marine Corps Cybersecurity Work Force

During the conduct of this research, ISSMs reported having as many as 10 systems within their portfolio at a given time. This means that in addition to working new ATOs for systems in the design and development phases, they are simultaneously conducting annual security reviews for systems with current ATOs. Further, there are programs in development phase that would benefit significantly from cybersecurity expertise, but do not have these critical personnel assigned. Questions to illuminate this issue include: 1) How many programs are assigned under each Marine Corps ISSM and SCV as compared to other services? 2) What are average times to complete RMF steps across like programs among each of the services? 3) Does the current USMC cybersecurity work force have the capacity to complete all the work it is given in the aggregate? Our research revealed a deficiency in trained and certified personnel in key positions, which is potentially leading

to long delays in programs receiving an ATO. Further analysis of the Marine Corps' cybersecurity work force is needed to determine if it is sufficiently staffed to execute the Commandant's intent.

APPENDIX A. LEGAL FOUNDATIONS AND PUBLICATIONS

NIST SP 800-12 Rev. 1, "An Introduction to Information Security," describes the laws and publications that guide the use of the RMF:

- The *Federal Information Security Management Act (FISMA) 2002* was enacted as part of the E-Government Act of 2002 to address specific information security needs, which include, but are not limited to, providing: a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets; and the development and maintenance of minimum controls required to protect federal information and systems (as written in SEC. 301 of Public Law 107-347).
- The *Federal Information Security Modernization Act of 2014* was an amendment to FISMA that made several modifications to modernize federal security practices as well as promote and strengthen the use of continuous monitoring.
- [Office of Management and Budget] OMB Circular A-130, *Management of Federal Information Resources*, requires that federal agencies establish information security and privacy programs containing specified elements.
- FIPS 199 – *Standards for Security Categorization of Federal Information and Information Systems*, lists standards for the categorization of information and systems, which in turn provides a common framework and understanding of expressing security in a way that promotes effective management and consistent reporting.
- FIPS 200 – *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for information and systems that support the executive agencies of the Federal Government as well as risk-based process for selecting the security controls necessary to satisfy the minimum-security requirements.
- SP 800–18 – *Guide for Developing Security Plans for Systems*, describes the procedures for developing a system security plan, provides an overview of the security requirements of the system, and describes the controls in place or planned for meeting those requirements.
- SP 800–30 – *Guide for Conducting Risk Assessments*, provides guidance for conducting risk assessments of federal systems and organizations.

- SP 800–34 – *Contingency Planning Guide for Federal Information Systems*, assists organizations in understanding the purpose, process, and format of information system contingency plans (ISCPs) development with practical, real-world guidelines.
- SP 800–37 – *Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach*, provides guidelines for applying the Risk Management Framework to federal systems, including conducting the activities of security categorization, security control selection and implementation, security control assessment, system authorization, and security control monitoring.
- SP 800–39 – *Managing Information Security Risk: Organization, Mission, and Information System View*, provides guidelines to establish an integrated, organization wide program for managing information security risk to organizational operations (e.g., mission, functions, image, and reputation), assets, individuals, other organizations, and the Nation resulting from the operation and use of federal systems. SP 800–53, Security and Privacy Controls for Systems and Organizations, provides guidelines for selecting and specifying security controls for organizations and systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS Publication 200.
- SP 800-53 – *Security and Privacy Controls for Systems and Organizations*, provides guidelines for selecting and specifying security controls for organizations and systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS Publication 200.
- SP 800–53A – *Assessing Security and Privacy Controls in Systems and Organizations: Building Effective Assessment Plans*, provides (i) guidelines for building effective security assessment plans and privacy assessment plans; and (ii) a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in systems and organizations supporting the executive agencies of the Federal Government.
- SP 800–60 – *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists agencies in consistently mapping security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) systems (e.g., mission critical, mission support, administrative).
- SP 800–128 – *Guide for Security-Focused Configuration Management of Information Systems*, provides guidance for organizations responsible for managing and administrating the security of federal systems and associated environments of operation.

- SP 800–137 – *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, assists organizations in the development of an ISCM strategy and the implementation of an ISCM program, which provide awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls [26].

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. INTERVIEW QUESTIONS

Subject Background

- What branch of service or DOD agency are you or were you affiliated with?
    - How long have you been a part of that agency?
    - Other affiliations?
- Can you describe the role of your organization within that branch or agency?
- What is your job or billet title?
    - Where does your position/billet fall within the hierarchy of your organization?
- Can you describe the training you received prior to utilizing the Risk Management Framework?
    - Did you attend an in-person training or was it completed through an online tutorial?
    - Can you speak to your level of comfort with the process after you completed the training?

ATO Experiences

- Can you tell me about a time when you were involved with an ATO?
    - What was your role?
    - What authorities did you have within the process?
    - Who did you work with to complete the ATO process (more geared at process hierarchy)?
- Were contractors used as part of seeking the ATO or did your team do all the work?
    - Why did you decide to use/not to use contractors?
    - What did you tell the contractors to do?
    - Who managed the contractors?
    - How did you know if they were doing a good job?

- Can you describe the training you received prior to utilizing the Risk Management Framework?

    - Did you attend an in-person training or was it completed through an online tutorial?
    - Can you speak to your level of comfort with the process after you completed the training?
- Can you walk us through how you went about navigating the RMF?
    - Were there any steps of the RMF that cause significant delay as compared to others?
    - What aspects of the assess and authorize process are most time intensive?
    - How did you receive feedback throughout the RMF process and from whom?
- How did you go about completing all the paperwork throughout the process?
    - Did you create or work from an existing template?
    - Can you speak to how you determined which controls were relevant to your program?
- Was there a specific threat or security goal you (or your organization) were trying to mitigate?
- At what stage, with respect to the development of the system, was the RMF conducted?
    - Do you think this was most useful or accurate time to conduct the RMF?
    - Can you describe when might be a better time to conduct this process?

Risk/Threat Assessment

- Can you describe how you went about assessing the risks or threats to your program?
    - Was the assessment risk, threat, or compliance based?
    - Who was responsible for conducting the assessment?
    - What methods were used to determine this assessment?
    - Did the assessment borrow from previously approved ATOs from similar systems?
    - Was there an effort to validate the assessment that was made?

- Were benefits of the system or mission relevance ever cited as a reason not to select or implement a particular control?

Control Selection/Implementation

- How did you ensure the selected controls were implemented?
    - Who was responsible for ensuring the selected controls were implemented?
    - What factors drove the selection of particular controls?
        - Compliance vs. the threat assessment
- How was it determined that the selected controls adequately addressed the perceived risk?
- Were you able use part of an ATO that was approved for a similar system?
- Were you able to leverage risk mitigations inherited from the broader system or network?

RMF Speed and Alternative Processes

- Approximately how long did your ATO take?
    - How did you determine the beginning of the process?
- What do you think took the most time in your ATO process?
    - Threat assessment/control selection/control implementation/paperwork/ intermediate or final approvals
- If you had more resources, would that have helped speed up the process? If so, what resources?
    - Consulting vs. “in-house” expertise

RMF Perceptions

- Do you think the ATO reflects the security of your system?
    - Do you think your ATO reflects adequate security against new and evolving threats?
- Have you heard of any processes or techniques for improving RMF speed/ efficacy?

    - Did you consider using these alternatives in your project?
    - If not, what stopped you?
- Would you like to provide any final thoughts regarding your experience with the RMF or attaining an ATO?
    - Potential topics for future research/improvement
- Do you know any other individuals that might provide insights into utilizing the RMF?
    - Contact info

LIST OF REFERENCES

[1] Headquarters Marine Corps, "Commandant's planning guidance," United States Marine Corps, Washington, DC, USA, 2019 [Online]. Available: https://www.marines.mil/Portals/1/Publications/Commandant's%20Planning%20Guidance_2019.pdf?ver=2019-07-17-090732-937

[2] *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113–283*, 128 STAT. 3073*. 2014 [Online]. Available: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[3] "Department of Defense trusted computer system evaluation criteria," Department of Defense, Washington, DC, USA, DOD 5200.28-STD, 2005 [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/white-paper/1985/12/26/dod-rainbow-series/final/documents/std001.txt

[4] "DOD information technology security certification and accreditation process (DITSCAP)," Department of Defense, Washington, DC, USA, DOD Instruction 5200.40, 1997 [Online]. Available: https://www.acqnotes.com/Attachments/DOD%20Instruction%205200.40.pdf

[5] "Risk management framework (RMF) for DOD information technology (IT)," Department of Defense, Washington, DC, USA, DOD Instruction 8510.01, 2020.

[6] "Standards for security categorization of federal information and information systems," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST FIPS 199, 2004 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[7] "DOD information assurance certification and accreditation process (DIACAP)," Department of Defense, Washington, DC, USA, DOD Instruction 8510.01, 2007.

[8] Cybersecurity Policy Directorate, "DIACAP to risk management framework (RMF) transformation." Department of Defense, 2012 [Online]. Available: https://csrc.nist.gov/csrc/media/events/ispab-october-2012-meeting/documents/ispab_oct2012_dcussatt_dod-rmf-transition-brief.pdf

[9] "Minimum security requirements for federal information and information systems," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST FIPS 200, 2006 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[10] "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-53 Rev. 5, 2020. doi: 10.6028/NIST.SP.800-53r5.

[11] Office of the President of the United States, "Executive Order -- Improving Critical Infrastructure Cybersecurity." 2013 [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[12] "OMB Circular A-130, Office of Management and Budget," Washington, DC, USA, 2016 [Online]. Available: https://obamawhitehouse.archives.gov/node/15057

[13] "Risk management framework documentation, data element standards, and reciprocity process for national security systems," Center for the Development of Security Excellence, Ft Meade, MD, USA, CNSSI 1254, 2016 [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-1254.pdf

[14] Joint Task Force Transformation Initiative, "Risk management framework for information systems and organizations: A system life cycle approach for security and privacy," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-37r2, 2018 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[15] Headquarters Marine Corps, "Marine Corps authorization and assessment process," United States Marine Corps, Washington, DC, USA, USMC ECSM 018, 2020.

[16] "Security categorization and control selection for national security systems," Committee on National Security Systems, Ft Meade, MD, USA, CNSSI No. 1253, 2014 [Online]. Available: https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf

[17] L. de Castro *et al.*, "SCRAM: A Platform for Securely Measuring Cyber Risk," *Harv. Data Sci. Rev.*, 2020, doi: 10.1162/99608f92.b4bb506a.

[18] M. I. Heier and A. J. Morales, "Quantifying the risk management framework," M.S. thesis, Dept. of Info. Sciences, NPS, Monterey, CA, USA, 2020 [Online]. Available: https://calhoun.nps.edu/handle/10945/65543

[19] Chaplain, Christine T., "Weapon systems cybersecurity: DOD just beginning to grapple with scale of vulnerabilities," Washington, DC, USA, GAO Report No. GAO-19-128, 2018.

[20] C. Herley, "Unfalsifiability of security claims," *Proc. Natl. Acad. Sci.*, vol. 113, no. 23, 2016, doi: 10.1073/pnas.1517797113.

[21] R. Stevens *et al.*, "Compliance Cautions: Investigating Security Issues Associated with U.S. Digital-Security Standards," presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020. doi: 10.14722/ndss.2020.24003.

[22] Office of the Secretary of the Navy, "Cybersecurity readiness review," Department of the Navy, Washington, DC, USA, 2019 [Online]. Available: https://media.defense.gov/2020/May/18/2002301997/-1/-1/1/cybersecurityreview.pdf

[23] Y. Chun Tie, M. Birks, and K. Francis, "Grounded theory research: A design framework for novice researchers," *SAGE Open Med.*, vol. 7, Jan. 2019, [Online]. Available: http://journals.sagepub.com/doi/10.1177/2050312118822927

[24] R.S. Weiss, *Learning From Strangers: The Art and Method of Qualitative Interview Studies*. New York, NY, USA: The Free Press, 1995.

[25] C. Herley and P. C. Van Oorschot, "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit," in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, pp. 99–120. doi: 10.1109/SP.2017.38.

[26] "An introduction to information security," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-12r1, 2017. doi: 10.6028/NIST.SP.800-12r1.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California